#2

Docket No. 1573.1004/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Isamu YAMADA et al.

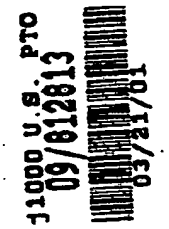
Serial No.:

Filed: March 21, 2001

For: INFORMATION DEVICE SYSTEM

Group Art Unit:

Examiner:



SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 2000-238968
Filed: August 7, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: March 21, 2001

By: _____
H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ８月 ７日

出 願 番 号
Application Number: 特願２０００－２３８９６８

出 願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 １月１９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１１３６４５

【書類名】　特許願

【整理番号】　0095101

【提出日】　平成12年 8月 7日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/76

H04B 7/24

【発明の名称】　情報機器システム

【請求項の数】　5

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　山田　勇

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　司波　章

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100105142

【弁理士】

【氏名又は名称】　下田　憲次

【電話番号】　078-936-1243

【手数料の表示】

【予納台帳番号】　011280

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9913421

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報機器システム

【特許請求の範囲】

【請求項１】　第１有線通信手段と第１無線通信手段とを、備えた第１情報機器と、

前記第１有線通信手段に接続されたとき前記第１有線通信手段と通信する第２有線通信手段と、前記第１無線通信手段と共に有効通信範囲内に存在するとき前記第１無線通信手段と通信する第２無線通信手段とを備える第２情報機器とを、具備し、前記第２情報機器が、更に、

前記第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２の無線通信手段が通信する無線通信状態であるか、前記有線通信状態及び無線通信状態以外の非通信状態であるかを判定する判定手段と、

この判定手段によって前記有線通信状態と判定されたとき、前記無線通信状態と判定されたとき、及び前記非通信状態と判定されたときの順で、前記第２情報機器が実行する処理の制限を大きくする制限手段とを、

備える情報機器システム。

【請求項２】　第１情報機器が備える第１有線通信手段と第２情報機器が備える第２有線通信手段とが接続されて、互いに通信する有線通信状態であるか、前記第１情報機器が備える第１無線通信手段と前記第２情報機器が備える第２無線通信手段とが有効通信範囲内に存在し、互いに通信する無線通信状態であるか、前記有線通信状態及び前記無線通信状態以外の非通信状態であるかを判定する判定段階と、

この判定段階において前記非通信状態と判定されたとき、前記無線通信状態と判定されたとき、前記有線通信状態と判定されたときの順で、前記第２情報機器が実行する処理の制限を大きくする処理制限段階とを、

具備する情報機器システムにおける処理制限方法。

【請求項３】　第１情報機器が備える第１有線通信手段に接続されたとき当該第１有線通信手段と通信する第２有線通信手段と、前記第１情報機器が備える第１無線通信手段と共に有効通信範囲内に存在するとき前記第１無線通信機器と通信

する第２無線通信手段とを、備える第２情報機器が読み取り可能な記録媒体であって、

前記第１及び第２有線通信手段が接続されて通信する有線通信状態であるか、前記第１及び第２の無線通信手段が通信する無線通信状態であるか、前記有線通信状態及び前記無線通信状態以外の非通信状態であるかを判定する判定ステップと、

この判定ステップによって前記非通信状態と判定されたとき、前記無線通信状態と判定されたとき、及び前記有線通信状態と判定されたときの順で、前記第２情報機器が実行する処理の制限を大きくする制限ステップとを、

備える記録媒体。

【請求項４】　第１有線通信手段と第１無線通信手段とを、備えた第１情報機器と、

前記第１有線通信手段に接続されたとき前記第１有線通信手段と通信する第２有線通信手段と、前記第１無線通信手段と共に有効通信範囲内に存在するとき前記第１無線通信手段と通信する第２無線通信手段と、ネットワークとの通信手段とを、備える第２情報機器とを、

具備し、前記第２情報機器が、更に、

前記第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２の無線通信手段が通信する無線通信状態であるか、前記有線通信状態及び無線通信状態以外の非通信状態であるかを判定する判定手段と、

前記ネットワークを介して他の情報機器に対してアウェアネス情報を通知すると共に、前記判定手段による判定結果に従って前記アウェアネス情報を変更する変更手段とを、

具備する情報機器システム。

【請求項５】　第１有線通信手段と第２無線通信手段とを備えた第１情報機器と、

第１有線通信手段に接続されたとき第１有線通信手段と通信する第２有線通信手段と、第１の無線通信手段が有効通信範囲内に存在するとき第１の無線通信手段と通信する第２の無線通信手段とを備える第２情報機器とを、

具備し、第１及び第２の有線通信手段による通信の伝送帯域が、第１及び第２の無線通信手段による通信の伝送帯域よりも広い情報機器システムにおいて、

第２情報機器は、

第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２無線通信手段が通信する無線通信状態であるかを判定する判定手段と、

前記有線通信状態であると前記判定手段で判定されたとき、第２の有線通信手段から第１の有線手段に情報を伝送させ、前記無線通信状態であると前記判定手段で判定されたとき、第２無線通信手段から第１無線通信手段に、データ量を減少させて前記情報を伝送させる制御手段とを、

具備する情報機器システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数の情報機器を有する情報機器システムに関し、特に各情報機器が有線通信機器及び無線通信機器を備えるものに関する。

【０００２】

【従来の技術】

複数台の情報機器間でのデータ伝送方式として、イーサーネット等を使用した有線ＬＡＮや、ＩＥＥＥ８０２．１１、ＩｒＤＡを利用した無線ＬＡＮが知られている。コンピュータで使用されるデバイスとコンピュータとの間の無線によるデータ伝送方式としては、Ｂｌｕｅｔｏｏｔｈが提案されている。同じくコンピュータで使用されるデバイスとコンピュータとの間での有線によるデータ伝送方式として、ＵＳＢ、ＰＣＭＣＩＡ、ＩＥＥＥ１３９４が知られている。このような有線による通信手段を備えたパーソナルコンピュータは一般的に普及している。また無線インターフェースを標準搭載したパーソナルコンピュータも安価に実現できる環境下にある。

【０００３】

【発明が解決しようとする課題】

無線によるデータ伝送では、空間的に離れた場所間で通信を行うことができる

。しかし、一般的には有線通信の方が無線通信よりも伝送帯域を広くとることができる。従って、無線のデータ伝送帯域では、データ量の多い情報の伝送には、長時間を要する。上記とは逆に、有線によるデータ伝送では、無線によるデータ伝送と同じデータ量を伝送する場合、伝送時間は短いが、空間的に離れた場所でデータ伝送を受けることができない。また、無線によるデータ伝送と有線によるデータ伝送とは、独立したものとして使用されており、両者を関連させて使用されていない。従って、無線伝送と有線伝送とがそれぞれ有する優れた特性を有効に利用できていなかった。

【０００４】

本発明は、無線通信時には無線の利便性を維持し、有線通信時には有線の利便性を維持した情報機器システムを提供することを目的とする。

【０００５】

【課題を解決するための手段】

本発明による通信機器システムは、第１有線通信手段と第１無線通信手段とを備えた第１情報機器を有している。この第１情報機器は、例えば携帯可能なものであることが望ましい。また、第２情報機器は、第１有線通信手段に接続されたとき第１有線通信手段と通信する第２有線通信手段と、第１無線通信手段と共に有効通信範囲内に存在するとき第１無線通信手段と通信する第２無線手段とを備えている。第２情報機器は、第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２の無線通信手段が通信する無線通信状態であるか、前記有線通信状態及び無線通信状態以外の非通信状態であるかを判定する判定手段と、この判定手段の判定結果に従って、第２情報機器が実行する処理の制限を変更する制限手段とを、備えている。第２情報機器が実行する処理としては、例えば、第２情報機器が備えるファイルの読み書き、第２情報機器が備えるアプリケーションの起動、ネットワークを介しての通信、インターネットへのアクセス等がある。これらの各処理に対して制限が行われている。即ち、情報機器に対するアクセス権が、有線通信状態、無線通信状態、非通信状態によって異なっており、有線通信状態から非通信状態に向かうに従ってアクセス権の制限が大きくなっている。

【０００６】

前記判定手段及び制限手段は、例２情報機器が読み取り可能な記録媒体に、例えば判定ステップ及び制限ステップとして記録することができる。判定ステップは、第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２の無線通信手段が通信する無線通信状態であるか、前記有線通信状態及び無線通信状態以外の非通信状態であるかを判定する。制限ステップは、判定ステップの判定結果に従って、第２情報機器が実行する処理の制限を変更する。この記録媒体から、これらステップが第２情報機器に読み込まれ、前記判定手段及び制限手段として機能する。

【０００７】

このように構成された情報機器システムでは、有線通信状態であるか、無線通信状態であるか、非通信状態であるかの判断が行われる。有線通信状態と判断されると、第１及び第２情報機器が、第１及び第２有線通信手段が接続されて通信しているので、第１情報機器を所持している使用者が、第２情報機器のそばにいて、使用者によって第２情報機器が操作される。従って、第２情報機器が実行する処理の制限が最も少ない状態とされる。また、無線通信状態と判断されると、第１及び第２情報機器が、第１及び第２無線通信手段を介して通信しており、第１情報機器を所持している使用者は、第２情報機器の近辺にいて、使用者の管理が及ぶ範囲内で、第２情報機器が第三者に使用される。従って、第２情報機器が実行する処理がある程度制限された状態にされる。非通信状態と判断されると、第１及び第２情報機器の間で、第１及び第２有線通信手段、第１及び第２無線通信手段のいずれによっても、通信が行われてなく、第１情報機器を携帯している使用者は、第２情報機器からかなり離れた場所にいて、第２情報機器に対する管理ができない状態で第２情報機器が使用されていると考えられる。従って、第２情報機器が行う処理が、最も制限される。このように、第１有線通信手段と第２有線通信手段とが接続されて、互いに通信する有線通信状態であるか、第１無線通信手段と第２無線通信手段とが有効通信範囲内に存在し、通信する無線通信状態であるか、前記有線通信状態及び前記無線通信状態以外の非通信状態であるかが判定段階で判定され、この判定段階において前記非通信状態と判定されたとき

、前記無線通信状態と判定されたとき、前記有線通信状態と判定されたときの順で、前記第２情報機器が実行する処理の制限を大きくする処理制限段階とが、実行される。

【０００８】

このように、本情報機器通信システムでは、第１情報機器を所持している使用者の存在位置によって第２情報機器に対するセキュリティのレベルを異ならせているので、パスワードや識別子を第三者に知られていても、第１情報機器を使用者が確実に管理している限り、第２情報機器の各種処理のうち第三者に実行されたくない処理が、誤って第三者に実行されることがない。

【０００９】

なお、上記の情報機器システムにおいて、前記制限手段は、第２有線通信手段に接続された第１有線通信手段が、第２有線通信手段と通信を許可されたものであるか判定する第１判定手段と、第２無線通信手段と通信している第１無線通信手段が第２無線通信手段と通信を許可されたものであるかを判定する第２判定手段とを、具備するものとすることができる。第１及び第２の判定手段も、第２情報機器が読み取り可能な記録媒体に記録された第１及び第２判定ステップが、第２情報機器によって読み取られることによって構成するものとできる。第１判定ステップは、第２有線通信手段に接続された第１有線通信手段が、第２有線通信手段と通信を許可されたものであるか判定し、第２判定ステップは、第２無線通信手段と通信している第１無線通信手段が第２無線通信手段と通信を許可されたものであるかを判定する。

【００１０】

このような情報機器システムは一般に量産される。従って、或る情報機器システムの第２情報機器が、他の情報機器システムの第１情報機器と、有線または無線で通信できただけで、或る情報機器システムの第２情報機器において実行される処理の制限が緩和されると、セキュリティを確保することができない。そこで、第１及び第２有線通信手段が通信を許可されたものであるか、また、第１及び第２無線通信手段が、通信を許可されたものであるかの判定を行っている。通信を許可されていない第１及び第２有線通信手段間の通信の場合や、通信を許可さ

れていない第１及び第２無線通信手段の通信の場合には、例えば非通信状態と判定された場合と同じ制限状態とされ、セキュリティが確保されている。

【００１１】

なお、第２情報機器がネットワークとの通信のための通信手段を有する場合、第２情報機器は、第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２無線通信手段が通信する無線通信状態であるか、前記有線通信状態及び無線通信状態以外の非通信状態であるかを判定する判定手段と、この判定手段の判定結果に従って、前記通信手段が前記ネットワークへ送信するアウェアネスを変更させる変更手段とを、備えるものに変更することができる。

【００１２】

この判定手段と変更手段も、第２情報機器が読み取り可能な記録媒体に記録された判定ステップと変更ステップとが、第２情報機器に読みとられることによって、実現することができる。判定ステップは、前記有線通信状態及び無線通信状態以外の非通信状態であるかを判定する。変更ステップは、判定ステップの判定結果に従って、前記通信手段が前記ネットワークへ送信するアウェアネスを変更させる。

【００１３】

第１情報機器を携帯している使用者が第２情報機器のそばにいて、第１情報機器の第１有線通信手段を第２情報機器の第２有線通信手段に接続すると、有線通信状態であると判定される。第１情報機器を携帯している使用者が第２情報機器から離れた場所にいるが、有効通信範囲内にいれば、無線通信状態であると判定される。第１情報機器を携帯している使用者が有効通信範囲外にいると、非通信状態であると判定される。このような判定結果に従って、異なるアウェアネスがネットワークに送信される。このように、第１有線通信手段と第２有線通信手段とが通信する有線通信状態であるか、第１無線通信手段と第２無線通信手段とが通信する無線通信状態であるか、前記有線通信状態及び前記無線通信状態以外の非通信状態であるかが、判定段階で判定される。この判定段階における判定結果に従って、変更段階で前記第２情報機器からネットワークへのアウェアネスを変更される。

【００１４】

上記のようにして変更されたアウェアネスを、ネットワークを利用して第２情報機器と通信している第三者が知ることによって、第１情報機器を携帯している使用者が、どのような位置にいるかを知ることができる。

【００１５】

本発明による他の情報機器システムは、第１及び第２の情報機器を有している。第１情報機器は携帯できるものであることが望ましい。第１情報機器は、第１有線通信手段と第２無線通信手段とを備え、第２情報機器は、第１有線通信手段に接続されたとき第１有線通信手段と通信する第２有線通信手段と、第１の無線通信手段と共に有効通信範囲内に存在するとき第１の無線通信手段と通信する第２の無線通信手段とを備えている。第１及び第２の有線通信手段による通信の伝送帯域は、第１及び第２の無線通信手段による通信の伝送帯域よりも広い。第２情報機器は、第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２無線通信手段が通信する無線通信状態であるかを判定する判定手段と、前記有線通信状態であると前記判定手段で判定されたとき、第２の有線通信手段から第１の有線通信手段に情報を伝送させ、前記無線通信状態であると前記判定手段で判定されたとき、第２無線通信手段から第１無線通信手段にデータ量を減少させて前記情報を伝送させる制御手段とを、備えている。前記情報は、例えば画像データ、音声データまたはこれら双方のデータを含むものである。データ量の減少は、例えばデータ圧縮技術を利用して行われる。

【００１６】

前記判定手段及び制御手段は、第２情報機器が読み取り可能な記録媒体に、判定ステップと、制御ステップとを記録し、これを第２情報機器が読み取ることによって実現できる。判定ステップは、第１及び第２有線通信手段が通信する有線通信状態であるか、第１及び第２無線通信手段が通信する無線通信状態であるかを判定する。制御ステップは、前記有線通信状態であると前記判定手段で判定されたとき、第２の有線通信手段から第１の有線通信手段に情報を伝送させる有線伝送ステップと、前記無線通信状態であると前記判定手段で判定されたとき、第２無線通信手段から第１無線通信手段にデータ量を減少させて前記情報を伝送さ

せる無線伝送ステップとを、備える。

【００１７】

本態様の情報機器システムでは、第１無線通信手段と第２無線通信手段とが有効通信範囲内に存在し通信する無線通信状態であるか、第１有線通信手段と第２有線通信手段とが接続され通信し、伝送帯域が前記無線通信状態よりも広い有線通信状態であるかが、判定段階で判定される。この判定段階において前記有線通信状態であると判定されたとき、有線伝送段階が、第２の有線通信手段から第１有線通信手段に情報を伝送させる。前記判定段階において前記無線通信状態であると判定されたとき、無線伝送段階が、前記第２無線通信手段から第１無線通信手段に、データ量を減少させて前記情報を伝送させる。

【００１８】

第１情報機器の第１有線通信手段が第２情報機器の第２無線通信手段に接続されていると、有線通信状態であると判定される。これによって、第２の有線通信手段から第１の有線通信手段に情報の伝送が行われる。即ち、広い伝送帯域を利用して情報の伝送が行われるので、データ量が多い情報であっても障害なく伝送され、必要且つ充分な情報を得ることができる。第１及び第２無線通信手段が無線通信状態にあると判定されると、第２の無線通信手段から第１の無線通信手段に、データ量を減少させて情報の伝送が行われる。即ち、狭い伝送帯域であっても、最低限度の情報を得ることができる。しかも、第１及び第２情報機器が離れた位置にあっても、この最低限度必要な情報を得ることができる。このように本態様の情報機器システムでは、無線接続時には無線の利便性を維持しつつ、最小必要限の情報が得られ、かつ有線接続時には必要充分な情報が得られる。

【００１９】

【発明の実施の形態】

本発明の第１実施形態の情報機器システムは、図１に示すように、第１情報機器、例えば端末機器２と、第２情報機器、例えばパーソナルコンピュータ４とを、備えている。

【００２０】

端末機器２は、図１に示すように、使用者が携帯可能な小型のカード型のもの

である。この端末機器２は、図２に示すように、マイクロプロセッサ６を有している。マイクロプロセッサ６は、第１有線通信手段、例えばＵＳＢインターフェース８と、第１無線通信手段、例えばＢｌｕｅｔｏｏｔｈ用の送受信回路１０とに接続されている。ＵＳＢインターフェース８は、図１に示すＵＳＢコネクタ８ａに接続されている。マイクロプロセッサ６は、内蔵するプログラムメモリに記憶されているプログラムに従って、ＵＳＢインターフェース８、送受信回路１０を制御する。なお、送受信回路１０及びＵＳＢインターフェース８を通じて得られたデータは、記憶手段、例えばフラッシュメモリ１２に格納される。この端末機器２は、マイクロプロセッサ６等を作動させるための電池１４も内蔵している。

【００２１】

パーソナルコンピュータ４は、図３に示すように、ＣＰＵ１６、ハードディスク、フロッピィディスクドライブ及びＣＤＲＯＭドライブ等からなるドライブユニット１８、キーボードやマウス等で構成される入力ユニット２０、メモリ２２、表示ユニット２４を有するものである。さらに、パーソナルコンピュータ４は、通信ユニット、例えばＬＡＮユニット２６を有し、ＬＡＮ等のネットワークとの通信が可能である。また、パーソナルコンピュータ４は、第２有線通信手段、例えばＵＳＢ制御器２８と、第２無線通信手段、例えばＢｌｕｅｔｏｏｔｈ用の送受信回路３０とを備えている。この送受信回路３０は、端末機器２が、予め定めた有効通信範囲内に存在するとき、端末機器２の送受信回路１０と通信が可能なものである。ＵＳＢ制御器２８は、パーソナルコンピュータ４の表面に設けたＵＳＢコネクタ２８ａに接続されている。パーソナルコンピュータ４は、ハードディスク８に記憶されているオペレーティングシステムの制御下で動作する。パーソナルコンピュータ４は、図１に示すような記録媒体、例えばＣＤＲＯＭ３２に記録されているプログラムを、ドライブユニット１８中のＣＤＲＯＭドライブを介してハードディスク８に読み込み、このプログラムを実行する。

【００２２】

図１に示す端末機器２のＵＳＢコネクタ８ａを、パーソナルコンピュータ４のＵＳＢコネクタ２８ａに接続することによって、端末機器２とパーソナルコンピ

ュータ４とは、有線通信可能となる。また、端末機器２がパーソナルコンピュータ４と離れた位置にある場合、ＵＳＢによる有線通信は不可能であるが、パーソナルコンピュータ４の無線送受信回路３０の有効通信範囲内に端末機器２がある場合、端末機器２の無線送受信回路１０とパーソナルコンピュータ４の無線送受信回路３０とによって無線通信が可能となる。無論、端末機器２が、上記有効通信範囲外にあるとき、無線通信は不可能である。

【００２３】

例えば端末機器２と共に販売されたＣＤＲＯＭ３２から読み込まれたプログラム（状態管理ソフト）は、メモリ２２に常駐しているもので、種々のイベントが発生するごとに開始される。なお、端末機器２とパーソナルコンピュータ４とが無線または有線で接続されたとき、または有線若しくは無線の接続が切断されたときにも、イベントが発生する。

【００２４】

この状態管理ソフトでは、図４に示すようにまず有線接続が行われているか否かが判断される（ステップＳ２）。これは、例えば、この状態管理ソフトを開始させたイベントが、ＵＳＢ接続が行われたことによって発生したものであるか否かを、イベントに付属するパラメータを判断することによって行える。

【００２５】

有線接続が行われていると判断されると、識別子の判定が行われる（ステップＳ４）。この識別子の判別では、パーソナルコンピュータ４に接続された端末機器２のＵＳＢから送信されてきた識別子が、このパーソナルコンピュータ４と通信を許可された端末機器の識別子であるか否か判別される。有線通信が許可されている識別子は、予めメモリ２２にデータとして記憶されているので、このデータを参照して、識別子の判別を行う。

【００２６】

識別子の判別の結果、通信を許可された端末機器でないと判別されると、状態管理ソフトはその処理を終了する。従って、パーソナルコンピュータ４との通信を許可されていない者が持っている端末機器２によって、パーソナルコンピュータ４が使用されることを防止できる。識別子の判別の結果、通信を許可された端

末機器であると判別されると、セキュリティレベルがＣであることを、オペレーティングシステムに通知し（ステップＳ６）、この状態管理ソフトの処理が終了する。

【００２７】

ステップＳ２において有線接続でないと判断されると、無線接続であるか否かが判定される（ステップＳ８）。これも、この状態管理ソフトを起動したイベントが無線通信による接続が行われたことによって発生したものであるか否かを、イベントに付属するパラメータから判断することによって行える。

【００２８】

無線接続が行われていると判断されると、識別子の判定が行われる（ステップＳ１０）。この識別子の判別では、パーソナルコンピュータ４に接続された端末機器２から無線通信によって送信されてきた識別子がこのパーソナルコンピュータ４との通信を許可された端末機器２の識別子であるか否かの判別が行われる。無線通信が許可されている識別子は、予めメモリ２２にデータとして記憶されているので、このデータを参照して、この判別が行われる。

【００２９】

識別子の判別の結果、通信を許可された端末機器でないと判別されると、状態管理ソフトは終了する。従って、パーソナルコンピュータ４との通信を許可されていない者が持っている端末機器２によって、パーソナルコンピュータ４が使用されることを防止できる。識別子の判別の結果、通信を許可された端末機であると判別されると、セキュリティレベルがＢであることを、オペレーティングシステムに通知し（ステップＳ１２）、この状態管理ソフトの処理が終了する。

【００３０】

ステップＳ８において無線接続でないと判断されたとき、オペレーティングシステムにセキュリティレベルがＡであることが通知され、この状態管理ソフトの処理が終了する。

【００３１】

この状態管理ソフトでは、有線接続でないと判断された後に、無線接続であるか否かの判断が行われているので、有線接続と無線接続とが同時に行われた場合

、有線接続であるとの判断が優先され、セキュリティレベルＣの通知がなされる。ステップＳ２及びＳ４が判定手段に相当し、ステップＳ４、Ｓ６、Ｓ１０、Ｓ１２、Ｓ１４が制限手段に相当する。

【００３２】

このセキュリティレベルの通知に従って、パーソナルコンピュータ４が行う様々な処理が制限される。例えば、ファイルアクセスがセキュリティレベルによって制限される場合には次のようになる。

【００３３】

セキュリティレベルＡの通知がオペレーティングシステムに対して行われると、オペレーティングシステムがパーソナルコンピュータ４をサスペンドさせるか、或いはスクリーンセーバーによって、第三者がパーソナルコンピュータ４にアクセスできないようにされる。

【００３４】

セキュリティレベルＢの通知がオペレーティングシステムに対して行われると、オペレーティングシステムは、先ずユーザーにログインを促す。このとき、正規のＩＤ及びパスワードからなるログイン情報が入力されないと、セキュリティレベルＡと同様に処理が行われる。正規のログイン情報が入力されると、セキュリティレベルＢに対応して予め定めたファイルへのアクセスが許可される。例えば各ファイルの読み出しのみが許可され、書き込みは許可されない。この他、特定のディレクトリにあるファイルについてのみ読み出し、書き込みが許可され、他のディレクトリにあるファイルについては読み出し、書き込みが許可されないようにすることもできる。

【００３５】

セキュリティレベルＣが通知されると、オペレーティングシステムは、ユーザーにログインを促す。ここで、上述した正規のＩＤ及びパスワードが入力されないと、セキュリティレベルＡと同様に処理が行われる。正規のＩＤとパスワードが入力されると、セキュリティレベルがＣであるので、アクセス権の制限が最も少ない状態とされる。例えば全てのファイルへの読み出し及び書き込みが可能となる。

【００３６】

また、ネットワークへのアクセスをセキュリティレベルＡ、Ｂ、Ｃによって制限することもできる。この場合、セキュリティレベルＡの通知がオペレーティングシステムに対して行われると、オペレーティングシステムがパーソナルコンピュータ４をサスペンドさせるか、或いはスクリーンセーバーによって、第三者がパーソナルコンピュータ４にアクセスできないようにされる。

【００３７】

セキュリティレベルＢの通知がオペレーティングシステムに対して行われると、オペレーティングシステムは、先ずユーザーにログインを促す。このとき、正規のログイン情報が入力されないと、セキュリティレベルＡと同様に処理が行われる。正規のログイン情報が入力されると、セキュリティレベルＢに対応して予め定めたネットワークへのアクセスが許可される。例えばファイルサーバー上の特定のファイルの読み出しのみが許可される。

【００３８】

セキュリティレベルＣが通知されると、オペレーティングシステムは、ユーザーにログインを促す。ここで、上述した正規のログイン情報が入力されると、セキュリティレベルがＣであるので、アクセス権の制限が最も少ない状態とされる。例えばファイルサーバー上の全てのファイルへの読み出し及び書き込みが可能となる。正規のログイン情報が入力されないと、セキュリティレベルＡと同様に処理が行われる。

【００３９】

また、起動できるアプリケーションをセキュリティレベルＡ、Ｂ、Ｃによって制限することもできる。この場合、セキュリティレベルＡの通知がオペレーティングシステムに対して行われると、オペレーティングシステムがサスペンドさせられるか、或いはスクリーンセーバーによって、第三者がパーソナルコンピュータ４にアクセスできないようにされる。

【００４０】

セキュリティレベルＢの通知がオペレーティングシステムに対して行われると、オペレーティングシステムは、先ずユーザーにログインを促す。このとき、正

規のログイン情報が入力されないと、セキュリティレベルＡと同様に処理が行われる。正規のログイン情報が入力されると、セキュリティレベルＢに対応して予め定めたアプリケーションの起動が許可される。

【００４１】

セキュリティレベルＣが通知されると、オペレーティングシステムは、ユーザーにログインを促す。ここで、上述した正規のＩＤ及びパスワードが入力されると、セキュリティレベルがＣであるので、全てのアプリケーションの起動が可能とされる。このとき、正規のログイン情報が入力されないと、セキュリティレベルＡと同様に処理が行われる。

【００４２】

ファイルアクセスやアプリケーションの起動許可を制限する場合、セキュリティレベルＢ、Ｃでは、ログインを促すのに代えて、スクリーンセーバーを起動すると共に、パスワードの入力を促し、パスワードが入力されたとき、スクリーンセーバーを停止し、セキュリティレベルに応じて、ファイルアクセスまたはアプリケーションの起動を許可してもよい。或いは、ファイルアクセスやアプリケーションの起動許可を制限する場合、セキュリティレベルＢ、Ｃでは、ログインやパスワードの入力を促さずに、直ちにセキュリティレベルに応じてファイルアクセスやアプリケーションの起動を許可してもよい。

【００４３】

また、ブラウザソフトウエアによって閲覧することができるコンテンツをセキュリティレベルＡ、Ｂ、Ｃによって制限することもできる。この場合、状態管理ソフトからの通知は、オペレーティングシステムではなく、ブラウザソフトウエアに対して行われる。ブラウザソフトウエアは、閲覧できるコンテンツの制御レベルを変更可能に構成されているので、セキュリティレベルＡが通知されると、閲覧不能に制御レベルを設定する。また、セキュリティレベルＢが通知されると、例えばセックス、暴力に関するウェブへのアクセスを禁止するように設定する。セキュリティレベルＣが通知されると、全てのウェブの閲覧が可能に制御レベルを設定する。

【００４４】

また、チャットアプリケーションによる通信状態を制御することもできる。この場合も、状態管理ソフトからの通知は、オペレーティングシステムではなく、チャットアプリケーションに対して行われる。チャットアプリケーションでは、セキュリティレベルＡが通知されると、パーソナルコンピュータ４の使用者は不在である旨をチャットでの通信相手に通知する。また、セキュリティレベルＢが通知されると、使用者はパーソナルコンピュータ４の近辺にはいるが、席にはいない旨をチャットでの通信相手に通知する。セキュリティレベルＣが通知されると、パーソナルコンピュータ４の使用者は席にいる旨をチャットでの通信相手に通知する。このように通信相手へのアウェアネスの内容が、有線通信状態であるか、無線通信状態であるか、非通信状態であるかによって変更されている。

【００４５】

本発明の第２実施形態の情報機器システムは、図５に示すように、端末機器２ａの構成が、第１実施形態の端末機器２と相違する。即ち、端末機器２と同様に、マイクロプロセッサ６、ＵＳＢインターフェース８、送受信回路１０、フラッシュメモリ１２及び電池１４を備える他に、再生データ出力手段、例えば画像表示手段及び音声出力手段を備えている。画像表示手段としては、例えばＬＣＤ３２が使用され、音声出力手段としては、例えばスピーカ３４が使用されている。この他に再生データ生成手段として、音声入力手段を備えている。音声入力手段として、例えばマイクロホン３８が使用されている。

【００４６】

マイクロホン３８で集音された音声信号は、例えばＣＯＤＥＣ４０によって処理が施され、マイクロプロセッサ６に供給される。音声信号は有線若しくは無線通信によってパーソナルコンピュータ４に伝送される。

【００４７】

有線若しくは無線によってパーソナルコンピュータ４から伝送された音声信号は、ＣＯＤＥＣ４０によって処理が施され、スピーカ３４から出力される。同様に有線若しくは無線によってパーソナルコンピュータ４から伝送された画像信号は、マイクロプロセッサ６によって処理が行われ、ＬＣＤ３２によって表示される。

【００４８】

なお、パーソナルコンピュータ４においても同様に、端末機器２ａから有線若しくは無線によって伝送された音声若しくは画像信号の再生が可能なように構成されている。

【００４９】

例えば端末機器２ａと共に販売されたＣＤＲＯＭからパーソナルコンピュータ４のメモリ２２に読み込まれた伝送ソフトプログラムは、例えばパーソナルコンピュータ４から端末機器２ａに音声や画像等のデータを伝送しようとする場合に起動される。このソフトでは、第１実施形態のステップＳ２と同様に有線接続か否かの判断が行われる（ステップＳ２ａ）。有線接続であると判断されるとステップＳ４と同様に識別子の判断が行われる（ステップＳ４ａ）。パーソナルコンピュータ４との通信が許可された端末機器２ａが有線接続されていると判断されると、伝送しようとするデータの広帯域伝送が有線によって行われる（ステップＳ１６）。

【００５０】

ステップＳ２ａにおいて有線接続でないと判断されると、ステップＳ８と同様に無線接続であるか否かの判断が行われる（ステップＳ８ａ）。無線接続であると判断されると、ステップＳ１０と同様に識別子の判断が行われる（ステップＳ１０ａ）。パーソナルコンピュータ４との通信が許可された端末機器２ａが無線接続されていると判断されると、伝送しようとするデータの狭帯域伝送が無線によって行われる（ステップＳ１８）。

【００５１】

例えばテレビ会議のような画像と音声とを含む情報の場合、広帯域伝送では、画像信号と音声信号とをそのまま有線伝送する。これらのうち画像は、端末機器２ａにおいてＬＣＤ３２によって表示され、音声はスピーカ３４から拡声される。狭帯域伝送では、データ量を減少させて、例えば画質あるいはコマ数を落として画像信号を端末機器２ａに伝送し、音声信号も音質を下げて、端末機器２ａに伝送する。これらのうち画像がＬＣＤ３２によって表示され、音声はスピーカ３４から拡声される。

【００５２】

パーソナルコンピュータ４によってインターネットやデジタルテレビ放送から取得された画像信号や音声信号も、同様に有線通信では広帯域で、無線通信では狭帯域で、それぞれ端末機器２ａに伝送される。なお、画像信号のみ或いは音声信号のみを上記と同様に伝送することもできる。

【００５３】

また、端末機器２ａにも、上述した伝送ソフトが読み込まれており、マイクロホン３８で集音された音声信号は、有線通信の場合には広帯域伝送され、無線通信の場合には狭帯域伝送される。例えば、狭帯域伝送の場合、マイクロプロセッサ６によって音声信号は、テキストに変換され、このテキストによって伝送される。広帯域伝送の場合、音声信号がそのまま伝送される。或いは、端末機器２ａが音声メモとしての機能を備えていると、端末機器２ａのフラッシュメモリ１２に記憶された音声信号は、狭帯域伝送の場合、記憶されている音声ファイルの一部のみ日時時刻情報とパーソナルコンピュータ４に伝送される。また、広帯域伝送の場合、記憶されている音声ファイルの全てを伝送する。

【００５４】

上記の２つの実施形態では、有線通信手段としてＵＳＢを使用したが、他の有線通信手段、例えばＩＥＥ１３９４、ＰＣＭＣＩＡを使用することもできる。また、無線通信手段としてＢｌｕｅｔｏｏｔｈを使用したが、他の無線通信手段、例えば無線ＬＡＮを使用することもできる。第１実施形態では、図４の状態管理ソフトにおいて、セキュリティレベルＡ、ＢまたはＣをオペレーティングシステムに通知したが、これに代えて、オペレーティングシステムが適宜アクセスするメモリに、セキュリティレベルを書き込んでおくこともできる。第２実施形態では、端末機器２ａから音声信号のみを伝送するようにしたが、画像信号を伝送することもできる。この場合でも、無線通信の場合にはデータ量を減少させるように画質を落としたり、コマ数をおとした画像を伝送し、有線通信の場合には、データ量をそのままとして伝送する。

【００５５】

【発明の効果】

以上のように、本発明によれば、第１及び第２情報機器が、有線通信手段と無線通信手段とをそれぞれ有し、これらの間で有線通信が行われているときには第２情報機器に行わせることができる処理の制限を最も少なくし、無線通信が行われているときには処理の制限を高め、有線でも無線でも通信が行われていないときには、処理の制限を最も高めている。従って、第１情報機器を携帯した第２情報機器の使用者が、第２情報機器に対してどのような位置にいるかによって、第三者が第２情報機器を使用する状態を制限することができる。また、有線通信が行われているときと、無線通信が行われているときと、通信が確立されていないときとで、第２情報機器からネットワークへのアウェアネスを異ならせているので、第２情報機器の使用者が、どのような位置にいるかをネットワークを介して通信相手に報知することができる。また、本発明によれば、第１及び第２の情報機器が、有線通信手段と無線通信手段とを備え、無線通信手段では伝送帯域が狭く、有線通信手段では伝送帯域が広いので、有線通信が行われているときには、再生データを広帯域で伝送し、無線通信が行われているときには、データ量を減少させて情報を伝送している。従って、無線接続時には無線の利便性を維持しつつ、最小必要限の情報が得られ、かつ有線接続時には必要充分な情報が得られる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態の情報機器システムの全体構成図である。

【図２】

図１の情報機器通信システムで使用される端末機器のブロック図である。

【図３】

図１の情報機器システムで使用されるパーソナルコンピュータのブロック図である。

【図４】

図３のパーソナルコンピュータが実効する状態管理プログラムのフローチャートである。

【図５】

本発明の第２実施形態の情報機器システムで使用される端末機器のブロック図である。

【図６】

図５の情報機器システムで使用されるパーソナルコンピュータが実行する伝送プログラムのフローチャートである。

【符号の説明】

２　端末機器（第１情報機器）

４　パーソナルコンピュータ（第２情報機器）

８　ＵＳＢ（第１有線通信手段）

１０　送受信回路（第１無線通信手段）

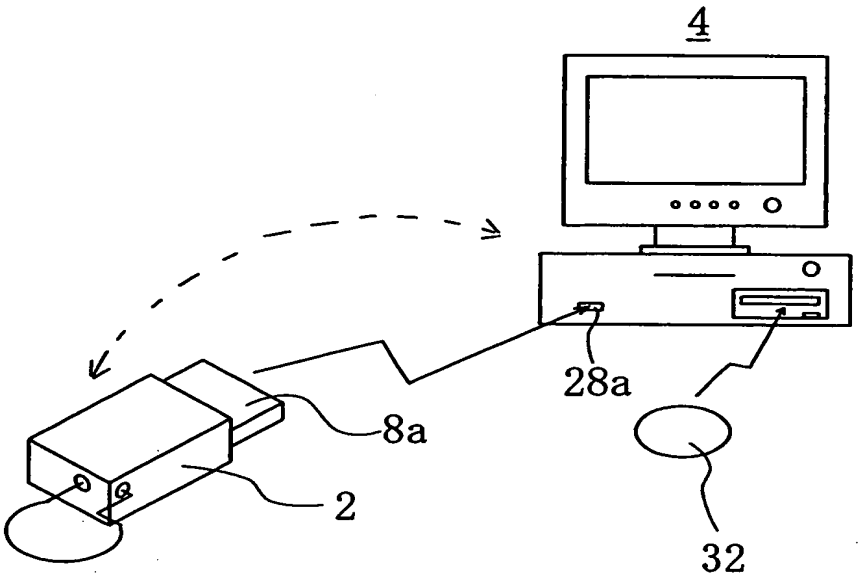
２８　ＵＳＢ制御器（第２有線通信手段）

３０　送受信回路（第２無線通信手段）

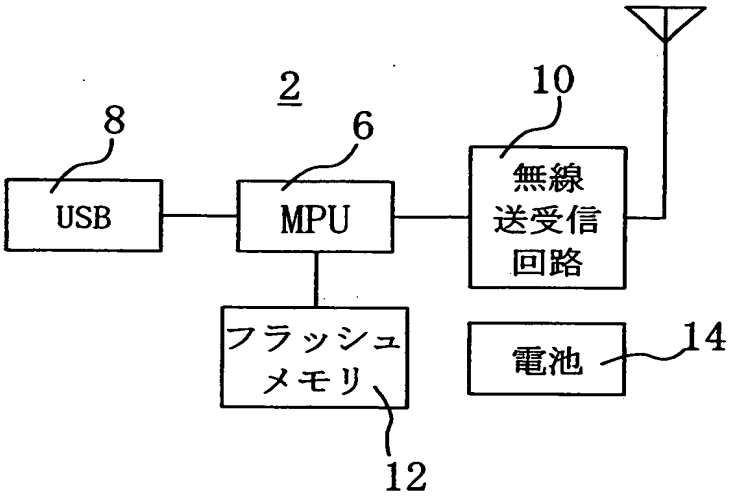
３２　ＣＤＲＯＭ（記録媒体）

【書類名】　図面

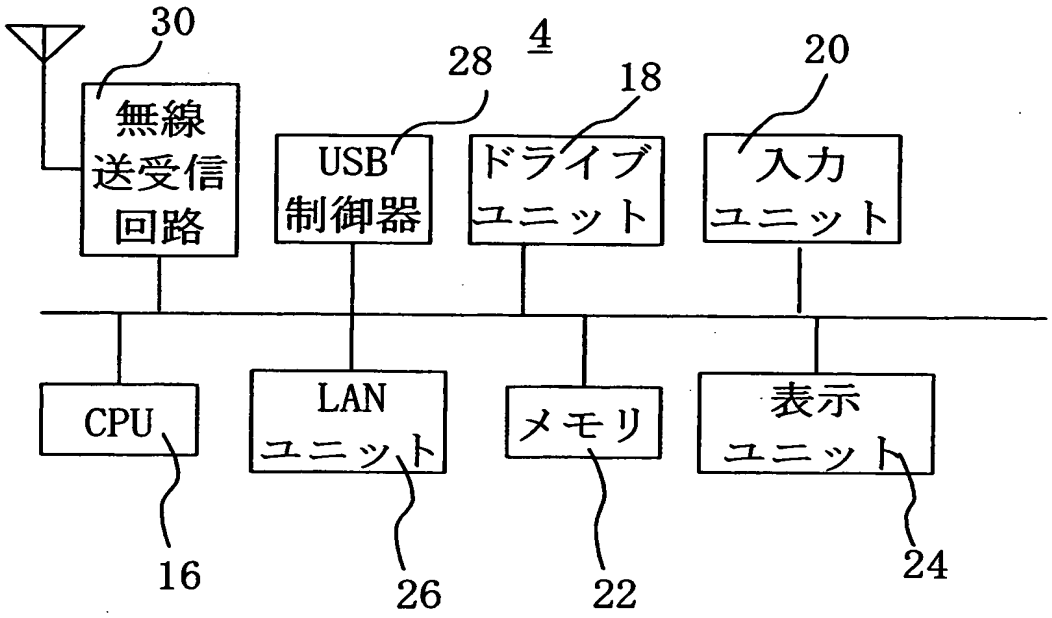
【図１】



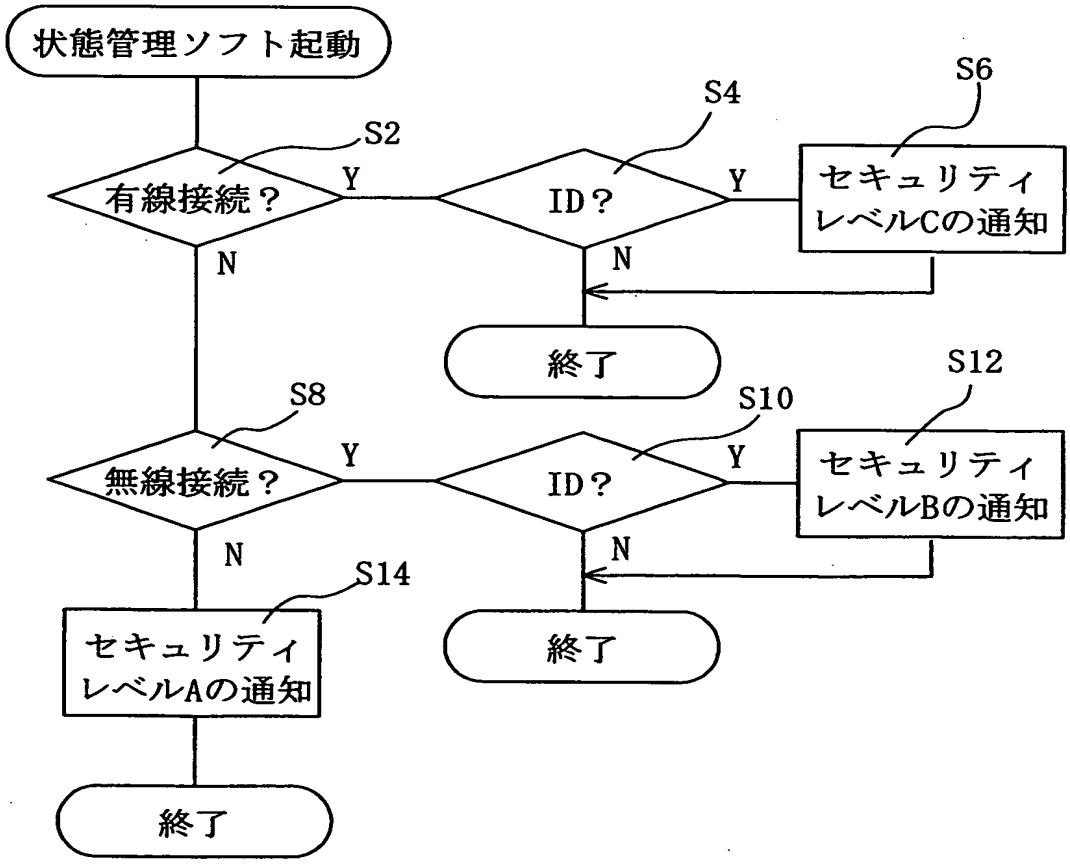
【図２】



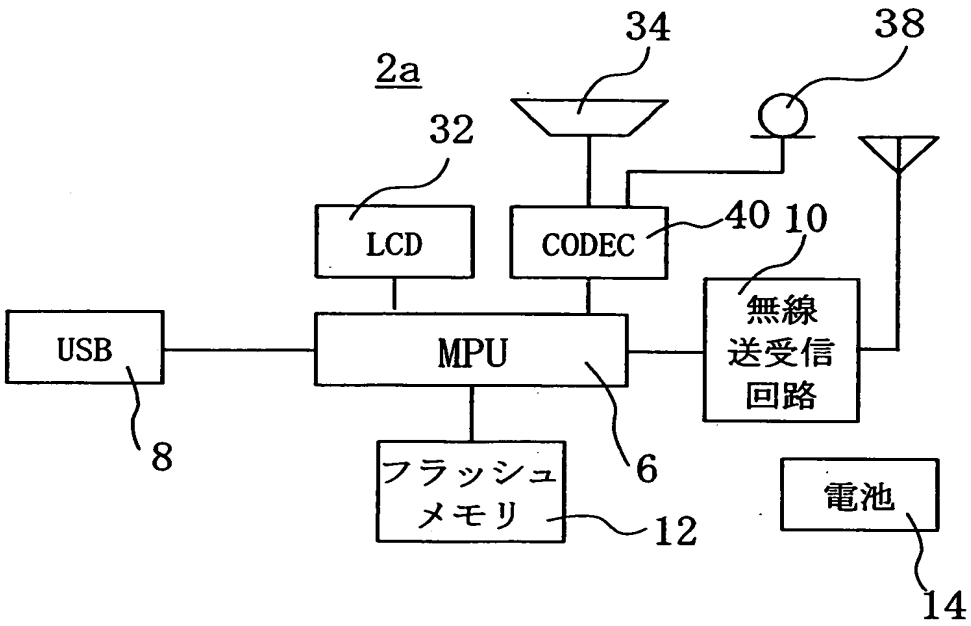
【図３】


4
30
無線
送受信
回路
28
USB
制御器
18
ドライブ
ユニット
20
入力
ユニット
CPU
LAN
ユニット
メモリ
表示
ユニット
16
26
22
24

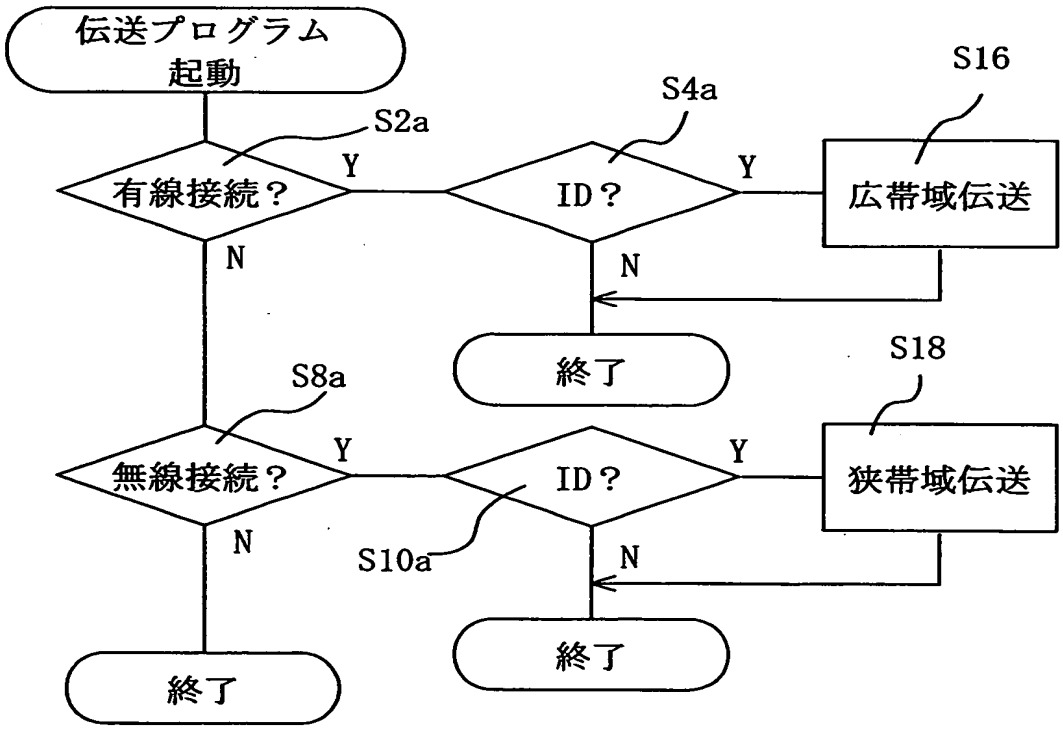
【図４】


状態管理ソフト起動
S2
有線接続？
Y
N
S4
ID？
Y
N
S6
セキュリティ
レベルCの通知
終了
S8
無線接続？
Y
N
S10
ID？
Y
N
S12
セキュリティ
レベルBの通知
終了
S14
セキュリティ
レベルAの通知
終了

【図５】


2a
34
38
32
LCD
CODEC
40
10
無線
送受信
回路
USB
MPU
8
6
フラッシュ
メモリ
12
電池
14

【図６】


伝送プログラム
起動
S2a
有線接続？
Y
N
S4a
ID？
Y
N
S16
広帯域伝送
終了
S8a
無線接続？
Y
N
S10a
ID？
Y
N
S18
狭帯域伝送
終了
終了

【書類名】　　要約書

【要約】

【課題】　情報機器のセキュリティレベルを情報機器の使用者がいる位置によって異ならせる。

【解決手段】　端末機器２がＵＳＢインターフェース８と無線送受信回路10とを備え、情報機器４が、ＵＳＢインターフェース８と接続されたとき通信するＵＳＢ制御器28と、無線送受信回路10に無線通信が可能な送受信回路30とを備えている。情報機器４が読み取り可能な記録媒体32には、有線通信状態であるか、無線通信状態であるか、非通信状態であるかを判定する判定ステップと、この判定ステップの判定結果に従って、前記非通信状態、前記無線通信状態及び前記有線通信状態の順で前記情報機器が実行する処理の制限を大きくする制限ステップとを、備えている。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５２２３〕

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社